Hastings Law Journal

Volume 28 | Issue 2 Article 6

1-1976

Garbage in, Gospel out: Establishing Probable Cause through Computerized Criminal Information Transmittals

Judith J. Rentschler

Follow this and additional works at: https://repository.uchastings.edu/hastings_law_journal

Part of the Law Commons

Recommended Citation

Judith J. Rentschler, *Garbage in, Gospel out: Establishing Probable Cause through Computerized Criminal Information Transmittals*, 28 Hastings L.J. 509 (1976).
Available at: https://repository.uchastings.edu/hastings_law_journal/vol28/iss2/6

This Note is brought to you for free and open access by the Law Journals at UC Hastings Scholarship Repository. It has been accepted for inclusion in Hastings Law Journal by an authorized editor of UC Hastings Scholarship Repository.

GARBAGE IN, GOSPEL OUT: ESTABLISHING PROBABLE CAUSE THROUGH COMPUTERIZED CRIMINAL INFORMATION TRANSMITTALS

> Our nation's current social developments harbor insidious evolutionary forces which propel us toward a collective Orwellian society. One of the features of that society is the utter destruction of privacy, the individual's complete exposure to the all-seeing, all-powerful police state. Government agencies, civilian and military, federal, state and local, have acquired miles and acres of files, enclosing revelations of the personal affairs and conditions of millions of private individuals. . . .
>
> . . . .
>
> The criminal histories in the Bureau one surmises, are collections of "raw" fact, received from many sources and recorded without evaluation. No doubt inaccuracy, error and even outright falsity infiltrate the files.[1]

Introduction: The NCIC—Computerized Law Enforcement

The National Crime Information Center (NCIC) is a federally[2] maintained computerized data bank designed to assist federal, state, and local law enforcement agencies to combat crime. It collects seven types of data: reports on stolen vehicles, securities, boats, articles, license plates, stolen or crime-involved guns, and "wanteds and warrants" of persons sought on felony charges. In addition, a separate division contains computerized criminal histories (CCH) of offenders.[3]

---

1. White v. State, 17 Cal. App. 3d 621, 631-32, 95 Cal. Rptr. 175, 181-82 (1971) (Friedman, A.P.J., dissenting and concurring).

2. The NCIC grew out of an experimental centralized computerized criminal justice system developed under the auspices of Project SEARCH (System for Electronic Analysis and Retrieval of Criminal Histories). Initially only twenty states participated. In November, 1971 control of the centralized system was transferred to the Attorney General of the United States under 28 U.S.C. § 534 (1970). Pursuant to 28 C.F.R. § 0.85 (1975), operation and management of the NCIC is the responsibility of the Federal Bureau of Investigation.

3. 1974 FBI ANN. REP. 21. For a general description of the data files and their use, see PROJECT SEARCH, INTERNATIONAL SYMPOSIUM ON CRIMINAL JUSTICE INFORMATION AND STATISTICS SYSTEMS (1974) [hereinafter referred to as INTERNATIONAL SYMPOSIUM]. The symposium conducted by Project SEARCH included presentations and papers by experts in the field of computerized criminal information systems, as well as by numerous representatives of police departments and criminal justice agencies which have utilized the NCIC and developed systems of their own. These published papers

Users of the NCIC include criminal justice agencies in all fifty states, Puerto Rico, and the District of Columbia, FBI field offices, nine other federal law enforcement agencies, and the Royal Canadian Mounted Police.[4]

Many states have computer systems of their own which are compatible with the NCIC and which store additional data.[5] There are also several multistate systems,[6] urban and county-wide systems,[7] and intercounty systems.[8] At least one source reports plans to develop a compatible computer system by Scotland Yard which would link via satellite with the NCIC.[9] There are, in fact, literally hundreds of computerized criminal information systems which connect with the NCIC, as well as hundreds more which, with minor program adjustments, are capable of

---

are excellent background reading for those particularly interested in technical aspects of computerized criminal information systems.

4. 1974 FBI ANN. REP. 21; A. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 147 (1971).

5. State and local criminal justice agencies usually maintain files similar to those of the NCIC, often to serve as a back-up to the NCIC. Many states include additional data not included in the NCIC, such as files of missing persons, misdemeanor warrants, and other entries not eligible for inclusion in the NCIC. PROJECT SEARCH, PRELIMINARY REQUIREMENTS ANALYSIS FOR CRIMINAL JUSTICE—LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEMS, at 4-35 to -37 (1974). Detailed descriptions of these systems may be found in various papers contained in INTERNATIONAL SYMPOSIUM, *supra* note 3. Examples of state-wide criminal information systems include Arizona's ACIC (Arizona Criminal Information Center); California's CJIS (California Justice Information System) and CLETS (California Law Enforcement Telecommunications System); Florida's FCIC (Florida Criminal Information Center); Michigan's LEIN (Law Enforcement Information Network); New York's NYSIIS (New York State Identification and Intelligence System); and Washington's ACCESS (A Central Computerized Enforcement Service System).

6. *E.g.*, ALECS (Automated Law Enforcement Communications System), covering Illinois, Indiana, Kentucky, Iowa, Michigan, Missouri, Ohio, and Wisconsin; and linking systems between Sacramento, California and Salem, Oregon, and between Sacramento, California and Carson City, Nevada. These cooperating systems seek to trace fleeing felons in adjacent states. PROJECT SEARCH, PRELIMINARY REQUIREMENTS ANALYSIS FOR CRIMINAL JUSTICE—LAW ENFORCEMENT TELECOMMUNICATIONS SYSTEMS 4-33 (1974).

7. *E.g.*, ALERT (Automated Law Enforcement Response Team) in Kansas City, Missouri; RAWWS (Regional Automated Want/Warrants System) in Los Angeles, California; and PIN (Police Information Network) in Alameda County, California. *Id.* at 3-15. Another state system is LOIS (Law Enforcement Operational Information System), a subsystem of the IMIS (Integrated Municipal Information System) in Charlotte, North Carolina. INTERNATIONAL SYMPOSIUM, *supra* note 3, at 81.

8. *E.g.*, CRISS (Columbia Regional Information Sharing System) serving four counties in Oregon and one in Washington; and REJIS (Regional Justice Information System) serving the five-county St. Louis, Missouri area. *Id.*

9. A. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 148 (1971).

linking with the NCIC.[10] This vast web will, in theory, make it impossible for the fleeing criminal to escape the law, for his record will follow him wherever he may hide.

This note will first describe the NCIC process and discuss why an arrest made pursuant to an NCIC transmission should be considered a warrantless arrest. Secondly, the note will consider whether the NCIC report, if it is not a valid arrest warrant, can itself constitute probable cause to arrest. Finally, inquiry will focus on what measures can be undertaken to utilize the vast potential of the NCIC, without invading individual rights and freedom.[11]

While the problem of establishing probable cause remains the same regardless of which computerized criminal justice information system responds to an officer's request for warrant information on his suspect, certain problems are especially acute for the NCIC. For instance, each state must develop its own plan for update and utilization of the data;[12] hence, procedures and the quality of data fed to the NCIC vary from state to state. Because of the intimate interrelation of the various component systems, the NCIC is plagued not only by errors within its own data banks, but also by errors and delays involving the other systems. An officer running a warrant check may not even know, in fact, whether the computerized data transmittal reflects information stored in the NCIC itself or some other interfaced system.[13] This note will focus on the NCIC, but the reader should bear in mind that a fault

10. *See* STAFF OF SUBCOMM. ON CONSTITUTIONAL RIGHTS OF SENATE COMM. ON THE JUDICIARY 93d Cong., 2d Sess., FEDERAL DATA BANKS AND CONSTITUTIONAL RIGHTS 32-34 (Comm. Print 1974). Indirect linkage could be accomplished by linkage to the NLETS (National Law Enforcement Telecommunications Service), which interfaces with the NCIC and other similar systems. Beddome, *The NLETS Upgrade*, INTERNATIONAL SYMPOSIUM, *supra* note 3.

11. The scope of this note is limited to use of computerized criminal information transmittals in establishing probable cause for arrest, and to improving the NCIC to enhance its reliability in establishing probable cause. Problems not discussed include use of the NCIC computerized criminal histories at bail setting, sentencing, and probation revocation hearings; use of the NCIC report to impeach witnesses at trial; and use of NCIC technology to develop investigative leads through analysis of criminal patterns and practices. Nor does this note touch on the many potential abuses resulting from disclosure of the NCIC report to credit agencies or employers, or other uses as authorized pursuant to state law.

12. 28 C.F.R. § 20.21-.25 (1975).

13. In a case in the Nevada federal district court, the court and all participants assumed that the warrant check was made through the NCIC. United States v. Mackey, 387 F. Supp. 1121 (D. Nev. 1975). In fact, after the opinion was reported, Judge Clary was informed by the director of the FBI that the erroneous transmission was made through CLETS, the comparable California system. Letter from Kenneth C. Cory, Federal Public Defender representing the defendant in *United States v. Mackey*, to Judith Rentschler, Oct. 7, 1975.

in any single component system constitutes a defect in the entire system.

How the NCIC Works

The operating concepts of the NCIC are simple. An officer on the beat enters identifying data for a suspect by radio or a mobile computer terminal. In 120 seconds or less,[14] a return from the computer recites the suspect's criminal record, including whether he is wanted for a crime. Similarly, an officer can enter the registration number of a vehicle or other identifiable article, and the computer return will indicate whether that article has been reported stolen. A single enquiry triggers a search of city, state, and multistate data banks as well as that of the NCIC. Through nationwide linkages, a criminal's record is made instantly available to the investigating officer, thereby enhancing the prospect of apprehension of criminals.

A hypothetical case best illustrates how the NCIC works. Suppose a burglary takes place in Detroit, Michigan, in which a 1967 Volkswagen is stolen. The Detroit police immediately enter the vehicle registration number in the stolen vehicles file of the NCIC. Fingerprints at the scene are sent to the FBI crime lab, and are there identified as those of Jack Smith. Based on this information and other investigation, a warrant is issued for Smith's arrest. The warrant is entered into the NCIC wanteds and warrants file. It is there retrievable under multiple identifying features, such as name, social security number, drivers license number, physical characteristics, known alias, etc.

Three weeks later an officer in Philadelphia stops Richard Roe on the road for a burnt out brake light. In the course of issuing a citation the officer takes Roe's license and the auto registration and performs a routine NCIC check through his mobile computer terminal. Roe has no criminal record, but the auto is identified as the vehicle stolen in Detroit. Roe and the car are taken into custody.

Still later, an officer in San Francisco stops Jack Smith carrying a toolbox in a residential area late at night. Smith's answers to routine questioning fail to satisfy the officer. He takes Smith's drivers license and performs a computer check while Smith waits. On confirmation of the outstanding Detroit warrant for Smith's arrest, Smith is arrested and returned to Michigan to face the charges there.

The crime has been solved; Smith has been brought to justice; and the victim's auto is restored. What's wrong with that?

14. NATIONAL ADVISORY COMMISSION ON CRIMINAL JUSTICE STANDARDS AND GOALS, CRIMINAL JUSTICE SYSTEM 39 (1973).

Suppose the reports returned from the NCIC had been wrong. Suppose the car had been recovered in the interim, and lent to Roe, but the police had failed to update the records. Or suppose that the Jack Smith stopped in San Francisco was a different Jack Smith, but the warrant reported by the NCIC had been incorrect, identifying the wrong person. Both innocent individuals would eventually be exonerated, to be sure, but not without damage. They may have spent time in jail, waiting for the mixup to unravel. And a criminal record may have been established and disseminated to other agencies, including employment or licensing agencies which may have access under state law,[15] before the error is corrected.

Ultimate conviction of the culprit does not by itself satisfy the Constitution. All the procedures leading to the apprehension and arrest of the criminal must meet the demands of the Constitution, especially that a person's liberty not be restrained, absent probable cause. If the NCIC does have the potential for error suggested above, the question arises whether the requirements of the fourth amendment are met where probable cause to arrest is based solely upon information transmitted by NCIC computers.

---

15. Access to the NCIC may be had under state or federal authority. Access is limited to official use by "authorized officials of the Federal Government, the States, cities, and penal and other institutions." 28 U.S.C. § 534(a)(2) (1970). Dissemination under state law to employers and licensing authorities was attacked and discussed in Menard v. Mitchell, 328 F. Supp. 718 (D.D.C. 1971). The court ruled that such dissemination was improper. But a portion of that holding was overruled by Congress in an appropriations act for 1972. Act of Dec. 15, 1971, Pub. L. No. 92-184, § 902, 85 Stat. 627, 642. The act provides: "[f]unds . . . may be used . . . for the exchange of identification records with officials of federally chartered or insured banking institutions to promote or maintain the security of those institutions, and, if authorized by State statute and approved by the Attorney General, to officials of State and local governments for purposes of employment and licensing, any such exchange to be made only for the official use of any such official and subject to the same restriction with respect to dissemination as that provided for [under the Justice Appropriations Act of 1972]." Dissemination of NCIC records is further regulated by 28 C.F.R. § 20.21 *et seq.* (1975), but authorized dissemination still depends in part on state law. And most states do authorize dissemination for employment and licensing purposes. *Hearings on H.R. 13315 Before Subcomm. No. 4 of the House Comm. on the Judiciary*, 92d Cong., 2d Sess., Ser. 27, pt. 1, at 65-66 (1972) (testimony of Richard Velde) [hereinafter cited as *Hearings on H.R. 13315*].

Dissemination of criminal records, whether or not computerized, to unauthorized individuals may have tragic consequences for the wronged individual. Yet federal sanctions for unauthorized dissemination are limited to cancellation of the privilege of use. 28 U.S.C. § 534(b) (1970). From 1924 to 1974, however, only six law enforcement agencies have been suspended for improperly making criminal records available. Menard v. Saxbe, 498 F.2d 1017, 1028 n.41 (D.C. Cir. 1974). States are free to adopt additional sanctions under 28 C.F.R. § 20.21 *et seq.* (1975).

United States v. Mackey

Ideally, of course, the NCIC reports would be infallibly accurate and would result in no infringement of the rights of innocent persons. But the accuracy of the NCIC is only a function of the diligence of the agencies utilizing the system, as *United States v. Mackey*[16] illustrates.

On October 24, 1974, James Mackey was stopped by police and asked for identification while hitchhiking[17] on Interstate 15 near North Las Vegas, Nevada. The police officer's radio warrant check[18] revealed a warrant outstanding for Mackey's arrest for probation violation in Monterey, California. Mackey was thereupon arrested for the probation violation, over his protest that the warrant had been fulfilled in May. A telephonic attempt to verify the warrant was unsuccessful because the transmission did not indicate which of three Monterey police departments had issued the warrant. During a routine search conducted as part of the booking process, an unregistered disassembled[19] twelve-gauge shotgun was discovered in Mackey's knapsack, a federal offense[20] for which Mackey was then also booked. Telegraphic verification of the Monterey warrant was then sought. A response the next day showed that, indeed, the warrant for probation violation had been satisfied in May, 1974. The probation violation charge was dropped. However, prosecution on the federal firearms violation proceeded in the United States District Court in Nevada. There, the court suppressed the evidence against Mackey—his disassembled shotgun—on the ground that it was the fruit of an unconstitutional arrest. The court based its decision on due process alone, citing the arbitrariness of the arrest, the "capricious disregard" of Mackey's rights, and the failure of the government to insure an "acceptable degree of accuracy" in the NCIC.[21] While these grounds would as easily have supported a decision based on the fourth amendment, the court mentioned the critical question whether the NCIC report constitutes probable cause for an arrest only in a cursory footnote:

16. 387 F. Supp. 1121 (D. Nev. 1975).

17. Hitchhiking is a violation of NEV. REV. STAT. § 484.331 (1973). However, the officers testified at trial that they would not have arrested Mackey for this violation, absent a "hit" from the NCIC. United States v. Mackey, 387 F. Supp. 1121, 1122 (D. Nev. 1975).

18. In *Mackey*, the officers and the court assumed that the warrant check had been made through the NCIC. See note 13 & accompanying text *supra*. Although the offending system was incorrectly identified, the impact of the court's decision remains unchanged.

19. Points and Authorities in Support of Defendant's Motion to Suppress at 3, United States v. Mackey, 387 F. Supp. 1121 (D. Nev. 1975).

20. Possession of an unregistered firearm violates 26 U.S.C. §§ 5861(c)-(d) (1970). Conviction carries a maximum penalty of $10,000 fine or ten years imprisonment, or both, for each violation. 26 U.S.C. § 5871 (1970).

21. 387 F. Supp. at 1125.

> The Court is cognizant of the Fourth Amendment basis for the arguments of counsel, but finds it unnecessary to focus on this line of analysis in order to reach a decision. Therefore, there is no need to resolve the issue of the status of NCIC as "reliable informant" so as to justify a warrantless arrest and search.[22]

The court, perhaps wisely, thus avoided basing its decision on fourth amendment grounds. But, in light of the rapid expansion of the criminal justice information network,[23] the question is certain to arise again. Ultimately, the traditional notions of probable cause must be examined anew in light of the failings of modern computer technology.

Framework of the Law of Arrest

The Fourth Amendment: Probable Cause

"[W]henever a police officer accosts an individual and restrains his freedom to walk away, he has 'seized' that person."[24] Protection against warrantless and unreasonable seizure is found in the fourth amendment, which provides a twofold guarantee: first, that a seizure not be unreasonable, and second, that a warrant will issue only upon probable cause.[25]

The United States Supreme Court has expressed a strong preference for arrests made under warrant.[26] But in *Gerstein v. Pugh*[27] the Court pointed out that it has never invalidated an arrest based on probable cause solely because the officer failed to obtain a warrant, so long as the issue of probable cause is submitted to a magistrate at a preliminary hearing promptly after the arrest.[28] In any event, probable cause must be determined in the neutral and detached judgment of a magis-

22. *Id.* at n.9.

23. In 1968, seven million transactions were made on the system. In 1973, forty million transactions were made. Sohn, Fielding, Foulkes & Granit, *Analysis and Traffic Projections for a National Law Enforcement Communications System*, INTERNATIONAL SYMPOSIUM, *supra* note 3, at 332. The NCIC contained 4.2 million records relating to wanted persons and stolen property in 1974, with an additional 400,000 computerized criminal histories maintained for criminal justice use. 1974 FBI ANN. REP. 21. Estimates of the total number of individuals eventually to be included in the system range from five to twenty million. HEW, REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS 232 (1973).

24. Terry v. Ohio, 392 U.S. 1, 16 (1968).

25. U.S. CONST. amend. IV. Probable cause has been defined as that state of facts and circumstances within the knowledge of the arresting officer and of which he has reasonably trustworthy information which warrant a man of reasonable caution in the belief that an offense has been or is being committed. Brinegar v. United States, 338 U.S. 160, 175-76 (1949); Carroll v. United States, 267 U.S. 132, 162 (1925).

26. Beck v. Ohio, 379 U.S. 96 (1964).

27. 420 U.S. 103 (1975).

28. *Id.* at 113-14.

trate—either before arrest through issuance of a warrant, or, in the case of a warrantless arrest, immediately after apprehension of the suspect.

Is the NCIC Transmission a Warrant?

In a footnote to the decision in *United States v. Mackey*, the district court assumed that an arrest based on an NCIC report is a warrantless one.[29] That assumption may, in fact, be rather rash. In states such as California, which authorize arrest as if under warrant based on telegraphically transmitted warrants or based on a warrant not in the possession of the arresting officer, the NCIC report might be considered analogous to these authorized procedures. However, the NCIC transmittal should not be considered a warrant, for it lacks safeguards of authenticity and freshness provided under these other procedures.

The United States Constitution does not define the term "warrant." Whether an arrest pursuant to an NCIC report is one made under warrant depends, then, on analogy to case law which has developed around more traditional forms of warrants and upon statutory requirements for the form of warrants. Although probable cause under the fourth amendment is a federal standard, the process of arresting a suspect for a state crime is largely governed by state law. This note will not attempt to survey the widely divergent state procedural laws, nor to apply these provisions to the use of computer technology in establishing probable cause. Instead, California law is used throughout this note as a convenient model of criminal procedure.

California law has developed fine distinctions between types of communications which may serve as a warrant for arrest. Police communications may be relied upon in California in establishing probable cause for arrest, but the degree of reliance which may be placed on such communications varies with the type of transmission. Arrest based on a telegraphic copy of a warrant or abstract of a warrant is considered an arrest made under warrant.[30] Arrest pursuant to a police communication that a warrant for arrest is outstanding is also an arrest under warrant.[31] But arrest based on a police communication

29. 387 F. Supp. 1121, 1125 n.9 (D. Nev. 1975).

30. CAL. PEN. CODE § 850 (West 1970 & Supp. 1976) provides: "A telegraphic copy of a warrant or an abstract of a warrant may be sent by telegraph, teletype, or any other electronic devices, to one or more peace officers, and such copy or abstract is as effectual in the hands of any officer, and he shall proceed in the same manner under it, as though he held the original warrant issued by a magistrate or the issuing authority or agency. . . ." Such a transmission will support arrest. Hewitt v. Superior Ct., 5 Cal. App. 3d 923, 85 Cal. Rptr. 493 (1970).

31. CAL. PEN. CODE § 842 (West 1970). *But see* People v. Webb, 66 Cal. 2d 107, 112, 424 P.2d 342, 345-46, 56 Cal. Rptr. 902, 905-06 (1967). In *Webb*, the court noted that police officers were entitled to proceed under a teletyped notice of a warrant outstanding for defendant's arrest, but also mentioned that such information provided

that the suspect is wanted is a warrantless arrest.[32]

The distinction among these types of communication is a vital one. An officer acting in good faith may rely without investigation on a warrant fair on its face, even if it later turns out to be false.[33] Police communications, on the other hand, while certainly an element to be considered in establishing probable cause, may or may not by themselves support an arrest, depending upon whether a warrant has been issued prior to arrest.[34]

Of the various types of communications, a telegraphically transmitted warrant[35] is the most reliable. The telegraphic warrant serves the traditional function of a warrant, that is, to insure that probable cause has been established by a magistrate. The telegraphic transmittal does not bear the signature of the magistrate, but the law which authorizes this type of warrant substitutes other guarantees of authenticity.

For instance, California Penal Code sections 850 and 851 authorize arrest under a telegraphically transmitted warrant or an abstract of a warrant. The telegraphically transmitted warrant must contain the following information:

> [T]he warrant number, the charge, the court or agency of issuance, the subject's name, address and description, the bail, the name of the issuing magistrate or authority, whether the offense charged is a felony or misdemeanor, and if the offense charged is a misdemeanor, whether the warrant has been certified for night service.[36]

A crucial safeguard is added by Penal Code section 851:

> Every officer causing telegraphic copies or abstracts of warrants to be sent, must certify as correct, and file in the telegraphic office from which such copies are sent, a copy of the warrant, and must return the original with a statement of his action thereunder.[37]

Although this section appears to afford adequate protection for transmittals, the safeguards provided may be substantially circumvented

---

reasonable cause for arrest, particularly when bolstered by the defendant's furtive conduct and attempted flight. *Id.*

32. *See* People v. Marguez, 237 Cal. App. 2d 627, 633, 47 Cal. Rptr. 170 (1965).

33. Herndon v. County of Marin, 25 Cal. App. 3d 933, 936-37, 102 Cal. Rptr. 221, 222-23 (1972).

34. Whiteley v. Warden, Wyo. State Pen., 401 U.S. 560 (1971); Remers v. Superior Ct., 2 Cal. 3d 659, 470 P.2d 11, 87 Cal. Rptr. 202 (1970); Ojeda v. Superior Ct., 12 Cal. App. 3d 909, 91 Cal. Rptr. 145 (1970); Hewitt v. Superior Ct., 5 Cal. App. 3d 923, 85 Cal. Rptr. 493 (1970).

35. Telegraphic warrants are authorized in California by CAL. PEN. CODE § 850 (West 1970 & Supp. 1976).

36. *Id.*

37. *Id.* § 851.

by proceeding under Penal Code section 842, as discussed below in detail.[38]

Upon execution of a traditional warrant, the officer must return the original warrant, with his action endorsed on the warrant, to the magistrate who issued the warrant.[39] Thus warrants which have been executed, and as to which no further action is required, are culled from the active files of the police agency. Telegraphic transmittal of stale and already executed warrants is avoided by requiring the officer to return the original warrant, with his action noted.

These safeguards present to the arresting officer certain minimum assurances that probable cause has already been established by a magistrate, and that the warrant is authentic and currently valid. However, these safeguards are not present in the NCIC report. The NCIC transmittal bears neither the certificate of the magistrate, as required on traditional warrants,[40] nor the certificate of the transmittor as required under Penal Code section 851. Transmittal by the NCIC is not accompanied by any reference to the original warrant, which is kept in the files of the issuing agency. Any activity on the warrant which affects its validity is not indicated in the NCIC transmittal unless the NCIC files have been altered by an update which adds notice of that activity to the file.

Update is the responsibility of the "user agency," the local law enforcement agency initiating the record in the computer.[41] Long delays in update are commonplace; delays of six months have been reported to be typical in some police departments.[42] As Nicholas Katzenbach testified before a House subcommittee on the Judiciary:

> In the city of New York, where I now live, and many other places, you simply cannot find out what has happened after an arrest was made.
>
> They have never caught up with it, it is never entered on the papers, it is floating up there in their estimation and never entered in, and you cannot discover the disposition of it.[43]

During the entire period of such a delay, regardless of any intervening events which may have invalidated the warrant, the NCIC reports a

38. See text accompanying notes 45-46 *infra*.

39. CAL. PEN. CODE § 828 (West 1970).

40. *Id.* § 814.

41. *National Crime Information Center Computerized Criminal History Program Background, Concept and Policy* at 2, 7 (approved April 1, 1976 by the NCIC Advisory Policy Board) [hereinafter cited as *NCIC Concept and Policy*].

42. The Philadelphia Police Department was six months behind in 1972, and getting further behind daily. *Hearings on H.R. 13315, supra* note 15, at 112-14 (testimony of Walter W. Cohen).

43. *Id.* at 5 (testimony of Nicholas Katzenbach).

valid outstanding warrant to all inquirers.[44] The absence of safeguards guaranteeing the authenticity and freshness of the NCIC reports should therefore preclude treating the NCIC as a telegraphically transmitted warrant.

A quite different type of police communication will also support an arrest made under warrant in California. Under Penal Code section 842, arrest pursuant to a warrant is lawful even though the officer does not have the warrant in hand.[45] Such an arrest is supported by none of the certification requirements of Penal Code sections 850 and 851, but rests only on the assertion of the police broadcaster that a warrant is outstanding. The inconsistency between sections 850 and 851 and section 842 is apparent, and renders the protection provided by the former two sections superfluous. The broadcaster proceeding under section 842 may completely avoid the certification requirements of sections 850 and 851, while the officer arresting on the basis of the information transmitted may proceed in precisely the same manner as if he had a warrant in hand.

Although the primary function of a warrant, establishment of probable cause, is served by arrest under notice of warrant pursuant to section 842, notice of warrant is inherently less trustworthy than a certified copy or abstract of a warrant. The NCIC fails, however, even to meet the lower standards of trustworthiness of a notice of warrant. A section 842 notice of warrant outstanding is accompanied by no cautionary instructions regarding its accuracy. It is presumed to be and is considered accurate as a police communication.[46] The NCIC transmission also indicates whether a warrant is outstanding. However, the NCIC notice is disclaimed by an accompanying warning to the officer to verify the information with the originating agency. In other words, the NCIC computer report notice is not "fair on its face," and therefore should not support an arrest without further investigation and verification.

Since an arrest based on an NCIC report fails to meet the requirements of arrests based on a warrant, it should be considered a warrantless arrest. The question remains, however, whether the NCIC report by itself may constitute probable cause for a warrantless arrest.

Probable Cause for a Warrantless Arrest

Grounds for a warrantless arrest were uniformly recognized at common law. Most states have codified them. Typical of state stat-

44. This is precisely what occurred in United States v. Mackey, 387 F. Supp. 1121 (D. Nev. 1975).

45. CAL. PEN. CODE § 842 (West 1970).

46. See text accompanying notes 30-37 *supra*.

utes is California Penal Code section 836, which permits an officer to effect a warrantless arrest:

> 1. Whenever he has reasonable cause to believe that the person to be arrested has committed a public offense in his presence.
> 2. When a person arrested has committed a felony, although not in his presence.
> 3. Whenever he has reasonable cause to believe that the person to be arrested has committed a felony, whether or not a felony has in fact been committed.[47]

In addition, California Penal Code section 1551.1 provides:

> The arrest of a person may also be lawfully made by any peace officer, without a warrant, upon reasonable information that the accused stands charged in the courts of any other State with a crime punishable by death or imprisonment for a term exceeding one year.[48]

The standard for making a warrantless arrest is the same under both sections 836 and 1551.1: "reasonable"[49] cause to believe that the suspect is a felon.

Police officers may rely on many factors in establishing probable cause. Most important, perhaps, is the evidence presented to their senses. In addition, they may consider information received through official channels, as well as tips from citizens or informants. The weight given any such source depends on the credibility that source has earned.[50]

By analogizing the NCIC report to, first, information received through official channels, and, second, to informants' tips, the NCIC's credibility may be more readily measured against the standard of probable cause required under the Constitution.

Official Channels

Information obtained through official channels deserves only slightly less reliance than a telegraphically transmitted warrant in es-

47. CAL. PEN. CODE § 836 (West 1970); *cf.* 18 U.S.C. § 3052 (1970) (authority of FBI agents to arrest without warrant).

48. CAL. PEN. CODE § 1551.1 (West 1970).

49. Reasonable cause is substantially synonymous with probable cause. Draper v. United States, 358 U.S. 307, 310 n.3 (1959); People v. Sanchez, 256 Cal. App. 2d 700, 704, 64 Cal. Rptr. 331, 334 (1967).

50. Where an officer seeks to rely on information obtained from an informant to support a warrantless arrest, it is essential that he present facts and circumstances justifying his belief that the informant is reliable. Spinelli v. United States, 393 U.S. 410 (1969). In addition, in his application for a warrant for arrest, or at the preliminary hearing following a warrantless arrest, the officer must present facts and circumstances justifying the conclusion of the informant that the suspect was engaged in criminal conduct; the conclusory statements of the informant are not sufficient of themselves to justify a warrantless invasion of privacy secured by the fourth amendment. *Id.*

tablishing probable cause. An officer may rely on such information to support a warrantless arrest;[51] but such an arrest, based on conclusory statements of another officer or agency, will be upheld only if the subsequent hearing on probable cause discloses that the officer communicating the report possessed knowledge of facts constituting probable cause.[52]

The case law on sufficiency of information obtained through official channels offers little assistance in deciding a case where, as in *Mackey*,[53] the official information is the sole cause of arrest.[54] Cases dealing with arrests based on official information generally involve situations where the official information is corroborated or supplemented by additional facts and circumstances. For instance, arrests have been upheld where: (1) the suspect had already aroused the attention and suspicion of the officers;[55] (2) the information relayed from the stationhouse was based on personal knowledge of a local police officer;[56] (3) an initial bulletin was subsequently corroborated by eyewitness observation of relevant detail;[57] or (4) exigent circumstances, such as im-

51. *E.g.*, People v. Ross, 67 Cal. 2d 64, 429 P.2d 606, 60 Cal. Rptr. 254 (1967) *rev'd on other grounds*, 391 U.S. 470; People v. Webb, 66 Cal. 2d 107, 424 P.2d 342, 56 Cal. Rptr. 902 (1967); People v. Honore, 2 Cal. App. 3d 295, 82 Cal. Rptr. 639 (1969).

52. Whiteley v. Warden, Wyo. State Pen., 401 U.S. 560 (1971); Remers v. Superior Ct., 2 Cal. 3d 659, 470 P.2d 11, 87 Cal. Rptr. 202 (1970).

53. United States v. Mackey, 387 F. Supp. 1121 (D. Nev. 1975).

54. Justification for detention so that officers may run a warrant check is difficult to imagine, absent some suspicious circumstances which would contribute to the determination of probable cause. Officers are not at liberty to detain individuals to determine if there are warrants outstanding against them. Barber v. Superior Ct., 30 Cal. App. 3d 326, 330, 106 Cal. Rptr. 304, 306 (1973).

In United States v. Mackey, 387 F. Supp. 1121 (D. Nev. 1975), the arresting officers testified that, absent a "hit" from the NCIC, they would not have arrested Mackey for the hitchhiking violation which constituted their threshhold reason for detention. *Id.* at 1122 n.2. Significantly, such activity resembles that condemned in Papachristou v. Jacksonville, 405 U.S. 156 (1972). In *Papachristou*, a vagrancy statute was found void for vagueness, in part because it authorized arbitrary "round-up" arrests which were a mere subterfuge for a conviction which could not otherwise have been obtained on the real but undisclosed grounds for the arrest. *Id.* at 169.

Nevertheless, police organizations resist legislation which would prohibit their running a warrant check absent specific and articulable grounds for suspecting that the individual is involved in criminal activity. *See, e.g.*, 11 THE PROSECUTOR 345-46 (1976).

55. *E.g.*, United States v. Golembiewski, 437 F.2d 1212 (8th Cir. 1971); People v. Honore, 2 Cal. App. 3d 295, 82 Cal. Rptr. 639 (1969); People v. Superior Court, 262 Cal. App. 2d 283, 68 Cal. Rptr. 629 (1968).

56. *E.g.*, United States v. Bell, 48 F. Supp. 986 (S.D. Cal. 1943); People v. Madden, 2 Cal. 3d 1017, 471 P.2d 971, 88 Cal. Rtpr. 171 (1970); People v. Lara, 67 Cal. 2d 365, 432 P.2d 202, 62 Cal. Rptr. 586 (1967).

57. *E.g.*, Restani v. Superior Court, 13 Cal. App. 3d 189, 91 Cal. Rptr. 429 (1970); People v. Schellin, 227 Cal. App. 2d 245, 38 Cal. Rptr. 593 (1964); People v. Borbon, 146 Cal. App. 2d 315, 303 P.2d 560 (1956).

minent peril of personal injury, called for immediate action.[58]

Generally, reliance on police radio broadcasts, hot sheets of local crimes, and similar official information is justified by the assumption that the information so obtained is highly reliable to a substantial certainty.[59] The risk of error, and consequent invasion of individual rights, is balanced against the officer's need to trust without question the information obtained from the stationhouse, particularly in potentially dangerous field situations.[60] Postarrest examination of the knowledge of the officer reporting the official information assures a high standard of accuracy, minimizing the risk of unreasonable seizure.

The NCIC, too, is an official channel through which information is received. But the automatically transmitted NCIC report represents the entire memory of the transmittor, and its cryptic and conclusory remarks represent the entire store of information relating to the facts and circumstances surrounding the warrant. The NCIC, as transmittor of the information pertaining to the suspect's criminal involvement, has no personal knowledge of the underlying facts and circumstances justifying its implicit recommendation that the suspect be arrested. Hence, no postarrest judicial examination of the "transmittor" of the official information is available to test the accuracy of the transmission or to encourage accurate transmittals.

As discussed above, reliance is justified by the assumption of accuracy; therefore, if the assumption of accuracy proves false, reliance is not justified. If the probability of incorrect information obtained through an official channel is substantial, then the constitutional requirement of probable cause is simply not met.

Statistical estimates of the NCIC's accuracy dramatize the fallacy of assuming that an NCIC report is reliable and an accurate basis for making an arrest. One commentator, after studying the operation of the NCIC in detail, estimates that the information maintained in and transmitted through the NCIC is 35 percent inaccurate.[61] While courts have repeatedly asserted that probable cause cannot rest on a formula of mathematical precision,[62] an officer who relies on an unverified

58. *E.g.*, People v. Hupp, 61 Cal. App. 2d 447, 143 P.2d 84 (1943).

59. *E.g.*, People v. Melchor, 237 Cal. App. 2d 685, 47 Cal. Rptr. 235 (1965); People v. Schellin, 227 Cal. App. 2d 245, 38 Cal. Rptr. 593 (1964).

60. *See, e.g.*, Note, *Field Interrogations: Court Rule and Police Response*, 49 J. URBAN L. 767 (1972).

61. DeWeese, *Reforming Our "Record Prisons": A Proposal for the Federal Regulation of Crime Data Banks*, 6 RUTGERS-CAMDEN L.J. 26, 33 (1974), *quoting* REPORT OF PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 604 (1968).

62. "In dealing with probable cause, . . . as the very name implies, we deal with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act."

NCIC transmission in making an arrest runs a known 35 percent risk that he thereby invades an innocent individual's right to be free from warrantless seizures. This high degree of error clearly makes reliance on unverified NCIC reports unreasonable. Arrests based on these reports therefore should not be tolerated under the Constitution.

Reliable Informants

Alternatively, the NCIC's status may be comparable to that of a reliable informant, a possibility raised by the district court in its footnote in the *Mackey* case.[63] Probable cause for arrest based solely on an informant's tip will support a warrant for arrest if the application for a warrant reveals both the factual bases for the conclusion of the informant and the underlying circumstances showing a reason to believe that the informant is credible.[64] Lacking either of these requirements, such a tip may be an element to consider in establishing probable cause, but some corroboration of the tip is required to support issuance of the warrant for arrest.[65]

The standard of probable cause is the same regardless of whether probable cause is determined prior to arrest at the application for a warrant, or after arrest at the preliminary hearing. But slightly less evidence may be required to establish probable cause where the determination is made by a magistrate prior to arrest than if it is made afterwards, on the rationale that the prearrest neutral determination by a magistrate is less likely to be tainted by the information which is obtained in the course of the warrantless arrest and search.[66] The quantum of proof required to establish probable cause applies as well to use of the NCIC at the preliminary hearing. An uncorroborated tip from a computerized informant found to be wrong one-third of the time should not support a warrant for arrest; *a fortiori*, it is inconceivable that it could support a warrantless arrest.[67]

The conclusion is obvious: probable cause requirements are not met if in fact the probability of error, and consequent invasion of innoent persons' rights, is as high as 35 percent. As the NCIC now operates, its transmissions should not constitute grounds for arrest without corroboration. When the NCIC is nearly 100 percent accurate, only the criminals' rights will be infringed. Until that time, however, the

Brinegar v. United States, 338 U.S. 160, 175 (1949); People v. Marquez, 237 Cal. App. 2d 627, 47 Cal. Rptr. 166 (1965).

63. United States v. Mackey, 387 F. Supp. 1121, 1125 n.9 (D. Nev. 1975).

64. Aguilar v. Texas, 378 U.S. 108 (1964).

65. *See* Spinelli v. United States, 393 U.S. 410 (1969); Draper v. United States, 358 U.S. 307 (1959).

66. *See* Wong Sun v. United States, 371 U.S. 471 (1963).

67. *See id.*; People v. Aguirre, 10 Cal. App. 3d 884, 89 Cal. Rptr. 384 (1970).

NCIC databank should only be used if the information transmitted is verified in some manner.

Recommendations for Reform

The district court in *United States v. Mackey*[68] recognized that a higher degree of accuracy than is currently maintained is essential if police seek to rely on the NCIC to support an arrest.[69] The *Mackey* court failed, however, to define an acceptable degree of accuracy.

Three distinct agencies must share the burden of improving the functions of the NCIC. First, the agency which issues the warrant for arrest must develop better procedures for updating and insuring the accuracy of information. Second, the arresting agency must, at least until the NCIC reporting system is improved, assume the responsibility for corroborating the information obtained through the NCIC before arresting on the basis of that report. And last, but most important, the NCIC itself must be improved to assist both the issuing and arresting agencies in update and corroboration duties and to establish uniform high standards for accuracy of its files.

Update: Keep Up the Input

Accuracy of input to the NCIC is the responsibility of the law enforcement agency which initiates a file.[70] But, as discussed above,[71] update lags uniformly exist. No federal sanctions are imposed to insure that the issuing agencies meet that responsibility.[72] State discipline of reporting procedures is not uniform.[73] The lack of firm enforcement of the federal update guidelines has resulted in a haphazard, nearly volunteer approach to updating the files.[74]

---

68. 387 F. Supp. 1121 (D. Nev. 1975).

69. *Id.* at 1125.

70. *NCIC Concept and Policy, supra* note 41, at 2, 7.

71. See notes 41-43 & accompanying text *supra.*

72. Dissemination of records to unauthorized persons may result in cancellation of use privileges. 28 U.S.C. § 534(b) (1970). But no sanctions for failure to update are available. Users are "encouraged" to update promptly, and the need for strict discipline has been recognized by the NCIC. *NCIC Concept and Policy, supra* note 41, at 3.

73. California law may serve as a model of necessary changes in the NCIC. In California, entry of disposition reports is mandatory under CAL. PEN. CODE §§ 11115-16, 11116.6-17 (West 1970 & Supp. 1976). Failure to do so may result in imposition of civil liability under CAL. GOV'T CODE § 815.6 (West 1970). Bradford v. State, 36 Cal. App. 3d 16, 111 Cal. Rptr. 852 (1973).

74. "Contributors of arrest cards are urged to submit followup information on the disposition of each arrest, but the FBI is not always successful in getting that information." *Hearings on H.R. 13315, supra* note 15, at 63 (testimony of Donald Santarelli). *See also id.* at 56-57 (testimony of Robert Gallati).

Reasons for this lack of concern for file accuracy are difficult to assess and cure. Where state law assigns the task of update to the police department itself,[75] the police claim that they suffer from delay in obtaining disposition reports from the courts.[76] Other departments bemoan understaffing and low budget allowances for this function.[77] Most difficult to solve is the loss of interest on the part of the local police after the case has been turned over to the prosecutor.[78]

These problems could be eliminated by assigning the task of update to the court involved in the disposition. This approach has been successful in some systems.[79] When the file is turned over to the prosecuting attorney, the police responsibility for input ends. The most efficient system includes on-line computer facilities maintained by the court which records all dispositions as they occur. The expense of this system may be prohibitive, however, and a less elaborate system of sharing the police department's terminal serves the same purpose at less cost.

One drawback to this alternative merits attention. It has been pointed out[80] that involving the courts so intimately in police computer systems may result in the appearance of a merging of the courts and executive police functions. This could have unpleasant effects on the integrity and independence of the courts. Judicial involvement in police systems presents two distinct problems. First, the use of inaccurate computerized police records at sentencing and like hearings may result in harsh sentences being imposed on the basis of erroneous information, to which the defendant may have no access or opportunity to correct the mistaken portions. Second, the independence of the courts must be maintained in order to protect the people from overzealous police activity. To overcome the potential ill effects of cooperation in

75. This system has been established in some computerized retrieval systems. *See* Rogers, *PROCES: An On-Line Case Management System for Prosecuting Attorneys*, INTERNATIONAL SYMPOSIUM, *supra* note 3, at 401 (discussion of the Honolulu program); *Hearings on H.R. 13315, supra* note 15, at 47-60 (testimony of Robert Gallati on the New York system).

76. *See, e.g., Hearings on H.R. 13315, supra* note 15, at 130 (testimony of Robert D. Gordon). As noted in the testimony of Robert Gallati, the courts are often under no legal duty to report dispositions to the police or law enforcement agencies. *Id.* at 56-57.

77. *See id.* at 112 (testimony of Walter Cohen); *id.* at 57 (testimony of Robert Gallati).

78. REPORT OF THE PRESIDENT'S COMMISSION ON LAW ENFORCEMENT AND ADMINISTRATION OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 268 (1967).

79. *See, e.g.*, Coundit, *Rochester Police Department Infosystem I*, INTERNATIONAL SYMPOSIUM, *supra* note 3, at 71; Feder, *Cable Car City's CABLE System, id.* at 468 (description of San Francisco Bay Area system).

80. Stern, *Considerations of Privacy, Confidentiality and Judicial Perspective in the Development of Court Computer Systems*, INTERNATIONAL SYMPOSIUM, *supra* note 3, at 499.

computerized record keeping, it is essential that the courts' access to the police computerized records system be strictly limited. Use of computer-generated police reports at sentencing and like hearings should be disallowed, especially until the NCIC files are accurate and the reports themselves are limited to those items truly probative of criminal involvement. This would preclude the courts' use of reports of arrests not followed by conviction at sentencing, parole revocation, and similar hearings, and would also prohibit use of such records at any hearing on application for an arrest warrant.

Corroboration: Crutch for a Weak System

Until the system is reliable, it is imperative that the arresting officer verify before arrest the information received from the NCIC. The officer must arrest on probable cause, based on information known at the time, or he must release his suspect. No intermediate course is allowed by the fourth amendment. Quite the opposite occurred in *Mackey*,[81] however. The difficulty faced by officers attempting to verify information is illustrated well by that case. The NCIC report acted somewhat as a referral to the issuing agency, without noting to which agency it referred. The transmittal in *Mackey* indicated that the warrant had issued from Monterey. It did not indicate which of the three police agencies in Monterey was responsible for the file.[82] After the officers attempted telephonic verification from one agency, they were instructed to proceed in the "usual manner," by booking Mackey and seeking telegraphic verification thereafter. Mackey was taken to jail at 5:45 P.M.; verification was not obtained until 9:00 A.M. the next day. Mackey thus sat in jail for fifteen hours before probable cause for his arrest was verified. This is clearly inappropriate under the fourth amendment.

In addition to the impediment created by the incomplete nature of an NCIC report, officers seeking verification of data are hindered by the mode of communication available. Telephonic corroboration of the warrant from the stationhouse was attempted in *Mackey*, but by then the suspect had already been arrested. Under the law, however, arrest on probable cause must be based on information known to the officer at the time of the arrest.[83] Corroboration must be made available to the officer on the beat, *before* arrest, rather than at the stationhouse afterwards. A combined radio-telegraphic system, as discussed

81. United States v. Mackey, 387 F. Supp. 1121 (D. Nev. 1975).

82. The three agencies are the Monterey City Police, the Park Police, and the Sheriff's Department.

83. Beck v. Ohio, 379 U.S. 89 (1964); Henry v. United States, 361 U.S. 98 (1959).

in detail below, could speed corroboration tremendously, and avoid prolonged delay in response.

Whatever mode of corroboration is used, the financial burden must be allocated equitably. It seems only fair that the cost of executing a warrant, including the cost of telephonic or radio-telegraphic corroboration, should fall on the issuing agency. That agency is thus spared the labor, expense, and risk of apprehending the suspect. Likewise, the issuing agency should bear the cost if, through its negligence, the file is not up-to-date or accurate.

If corroboration can be made easily available to the arresting officer, at no cost to his police force, the likelihood of making an arrest on the basis of inaccurate NCIC transmissions would be greatly reduced.

NCIC Modifications for Support of User Agencies

Redesign of the NCIC to facilitate update and corroboration would ease much of the burden imposed on user agencies. It would also enhance the overall effectiveness of the system.

Update

Update is, as discussed, the responsibility of the user agencies. The FBI "encourages" update by sending records of undisposed warrants to the issuing agency at ninety-day intervals, requesting verification. However, undisposed warrants remain in the system for one year,[84] notwithstanding failure of the originating agency to respond to a request for verification.

This lag presents a significant risk that inaccurate records will continue to be disseminated to requesting agencies. A simple record sealing program linked to the update request at the federal level would better serve to force prompt update. If no response is returned in ten days, the record would be sealed by the FBI. No further retrieval could thereafter be made until receipt of a current status report from the responsible agency.

Corroboration

Availability of a mode of corroboration and better identification of the issuing agency would assist arresting officers in verifying NCIC data before relying on it in making an arrest.

The NCIC can be programmed so that no warrant information

84. 28 C.F.R. § 20.33(a)(3) (1975) prohibits dissemination of undisposed arrest warrants more than one year old, for licensing, state or local employment, or other purposes.

could be transmitted unless linked with specific issuing agency information, including the telephone number of that agency. A change of this magnitude would require considerable additional manpower to add the information to existing files; the work would undoubtedly have to be done by local user agencies. These agencies already complain of overwork and understaffing.[85] These complaints, however, should not prevent improving the system for the benefit of the public.

Presently, corroboration must be made by the arresting agency communicating directly with the issuing agency. A nationwide linkage system, telegraphic or radio-telegraphic, could promote verification by reducing both cost and delay.[86] If the officer's warrant check produces a "hit" from the NCIC, the officer would request immediate verification through the NCIC, which would transmit his request to the originating agency. That agency would then respond with verification of the data to the NCIC, and thus to the officer.

Three advantages of this system are readily apparent. First, brevity of the initial NCIC response to an officer's inquiry is retained, while the opportunity is afforded for rapid expansion of the data if the report suggests cause for further inquiry. Second, verification could be made by the officer on the beat, via police callbox, patrol car radio, or teletype unit, routed through the stationhouse and thence through the NCIC switching system. Third, if the issuing agency's response fails to support the original information (the hit)—that is, if unrecorded alterations of the warrant affect its validity—the new data would automatically update the NCIC file. No subsequent arresting agency would be misled by inaccurate data.

Strenuous opposition to these changes could be expected from both the federal government and the user agencies. These modifications would certainly be expensive. A change in the system would require thousands of manhours, and a modification in the procedures of all the interfacing systems would be required as well.

Neither of these changes would *solve* the corroboration problem. No federal statute presently requires that the users verify the data at all; they are merely urged to do so. Modern computer technology has fostered a naive assumption that if a computer produced the report, it

85. *See, e.g., Hearings on H.R. 13315, supra* note 15, at 105, 112 (testimony of Walter W. Cohen); *id.* at 51, 57 (testimony of Robert Gallati).

86. A nationwide telegraphic linkage system known as NLETS (National Law Enforcement Telecommunications System, Inc.) currently serves as a direct link from the NLETS center in Phoenix, Arizona, and the capitals of the 48 adjacent states; it also links, through the NCIC, to Alaska, Hawaii, and Puerto Rico. However, this system is used principally for administrative messages. No inquiries of NCIC files are permitted through NLETS terminals. Beddome, *The NLETS Upgrade*, INTERNATIONAL SYMPOSIUM, *supra* note 3, at 441.

must be accurate;[87] and absent mandatory corroboration requirements, many officers will question neither the validity of that assumption nor the accuracy of the data received.

NCIC's Responsibility for Accuracy of the Files

In addition to requiring the NCIC to assist user agencies to update and corroborate by changing the resources available to users, the FBI, manager of the NCIC, must assume some independent responsibility for the accuracy of the NCIC files. Federal law does not adequately define the scope of the responsibility of the FBI for the data contained in the NCIC computers. Statutory authority to maintain the NCIC is couched in broad terms:

> (a) The Attorney General shall—
>
> (1) acquire, collect, classify, and preserve identification, criminal identification, crime, and other records; and
>
> (2) exchange these records with, and for the official use of, authorized officials of the Federal Government, the States, cities, and penal and other institutions.
>
> (b) The exchange of records authorized by subsection (a) (2) of this section is subject to cancellation if dissemination is made outside the receiving departments or related agencies.
>
> (c) The Attorney General may appoint officials to perform the functions authorized by this section.[88]

By regulation, responsibility for control of the NCIC is vested in the FBI in equally broad terms:

> Subject to the general supervision of the Attorney General, and under the direction of the Deputy Attorney General, the Director of the Federal Bureau of Investigation shall:
>
> . . .
>
> (b) Conduct the acquisition, collection, exchange, classification, and preservation of identification records, including personal fingerprints voluntarily submitted, on a mutually beneficial basis, from law enforcement and other governmental agencies, railroad police, national banks, member banks of the Federal Reserve System, FDIC-Reserve-Insured Banks, and banking institutions insured by the Federal Savings and Loan Insurance Corporation . . . .[89]

The extent of the FBI's responsibility under these sections has not been fully explored by the courts. The FBI has disclaimed responsibility for accuracy of the records it stores and disseminates, contending

87. *See* Baskir, *Data Banks and Privacy: A View from the Legislative Perspective*, in SYMPOSIUM: AUTOMATION IN THE COURTS, ITS IMPACT ON RECORD MAKING AND RECORD KEEPING 22 (1972).

88. 28 U.S.C. § 534 (1970).

89. 28 C.F.R. § 0.85 (1976).

that it is a mere passive recipient of them. In *Menard v. Saxbe*,[90] however, the District of Columbia Circuit specifically rejected this contention.[91] Specifically, the court found no duty to investigate the facts of remote arrests,[92] but the court ruled that when apprised that a police encounter does not constitute an arrest, the FBI must remove all record of that encounter from its criminal files, without formal request from the local agency.[93] Hence, records of detention short of arrest must be removed from the criminal files if the FBI has been informed of the true character of the detention.

The District of Columbia Circuit suggested further in *Tarlton v. Saxbe*[94] that the FBI cannot abrogate all responsibility for the accuracy of its files.[95] But that court declined to define what responsibility the FBI does have. That issue was left to be determined by later courts. None has yet done so.

The FBI is under an obligation to correct erroneous information contained in its records.[96] One court has suggested that the FBI may be required to notify all agencies to which it has sent erroneous information that such information is incorrect.[97] The FBI has also been required to expunge records of mass arrests.[98] Often, however, state law does not permit an individual a right of access to his police record. He may not know that a record exists, or that his existing record is incorrect, until the traffic officer who stops him for an auto inspection leans in the window and asks him to step out of his car.

Although federal legislation has been proposed, there is presently no federal law requiring expungement of records of arrest followed by dismissal of charges, or of records of arrest followed by acquittal. The courts have held that "[a]n arrest record, without more, is a fact which is absolutely irrelevant to the question of an individual's guilt."[99] But the police nevertheless consider these records indicative of criminal involvement[100] and oppose any system of expungement of records under

90. 498 F.2d 1017 (D.C. Cir. 1974).

91. *Id.* at 1026.

92. *Id.* at 1025.

93. *Id.* at 1028.

94. 507 F.2d 1116 (D.C. Cir. 1974).

95. *Id.* at 1123. *See also* Shadd v. United States, 389 F. Supp. 721 (W.D. Pa. 1975).

96. Chastain v. Kelley, 510 F.2d 1232 (D.C. Cir. 1975).

97. *Id.* at 1237.

98. *E.g.*, Sullivan v. Murphy, 478 F.2d 938 (D.C. Cir. 1973); Wilson v. Webster, 467 F.2d 1282 (9th Cir. 1972); United States v. McLeod, 385 F.2d 734 (5th Cir. 1967).

99. Utz v. Cullinane, 520 F.2d 467, 478 (D.C. Cir. 1975). *See also* Schware v. Board of Bar Examiners, 353 U.S. 232, 241 (1957).

100. *See, e.g., Hearings on H.R. 13315, supra* note 15, at 129-33 (testimony of Robert D. Gordon).

these circumstances.[101] A previous arrest, even if the disposition report indicates that the suspect was acquitted on constitutional or other grounds, will influence an officer running a warrant check on a suspect and may tip the scales in favor of arresting him.[102] These records must be expunged to prevent the bootstrapping effect of basing future arrests on the belief that an earlier, improper arrest indicates guilt.

Conclusion

Clearly, uniform standards of accuracy are essential if the computerized criminal information network is to be worthwhile. The high degree of error now pervading the system not only diminishes its effectiveness as a law enforcement tool but also threatens the rights of citizens who find themselves trapped in the indecipherable reels of a computerized record prison.

Congress has considered numerous bills which would alleviate the high risk of injury to individuals, while maintaining high standards for the system.[103] None has yet been passed. One bill[104] recently introduced by California Senator John Tunney would prohibit the investigating officer from running a warrant check absent specific, articulable grounds linking the suspect with criminal activity.[105] This alone would prevent the officer from arresting solely on the basis of the NCIC report.

The NCIC offers vast potential for good, but equal potential for abuse. And while it grows, monolithic and out of control, the potential for abuse grows apace.

*Judith J. Rentschler**

101. *See, e.g.*, 11 THE PROSECUTOR 345-46 (1976).

102. *See Hearings on H.R. 13315, supra* note 15, at 125 (testimony of Walter W. Cohen).

103. *E.g.*, S. 2964, 93d Cong., 2d Sess. (1974); S. 2963, 93d Cong., 2d Sess. (1974); H.R. 12574, 93d Cong., 2d Sess. (1974); S. 3633, 93d Cong., 2d Sess. (1974); H.R. 13315, 92d Cong., 2d Sess. (1972).

104. S. 2008, 94th Cong., 1st Sess. (1975).

105. This standard is comparable to the grounds for investigative detention set out in Terry v. Ohio, 392 U.S. 1 (1968).

* Member, Third Year Class.